SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

[METHOD OF INITIALIZING HYPER-FRAME NUMBERS DURING AN ESTABLISHMENT OF A NEW RADIO BEARER IN A WIRELESS COMMUNICATION SYSTEM]

Background of Invention

[0001] 1.Field of the Invention

[0002] The present invention relates to an initialization of hyper-frame numbers (HFNs) in a wireless communication system. In particular, the present invention discloses a method of initializing HFNs during an establishment of a new radio bearer.

[0003] 2.Description of the Prior Art

[0004] Please refer to Fig.1. Fig.1 is a simplified block diagram of a prior art wireless communications system, as defined by the 3rd Generation Partnership Project (3GPP) specifications 3GPP TS 25.322 V3.10.0 "RLC Protocol Specification", and 3GPP TS 25.331 V3.10.0 "Radio Resource Control (RRC) Specification", which are included herein by reference. The wireless communications system includes a first station 10 in wireless communications with a second station 20. As an example, the first station 10 is a mobile unit, such as a cellular telephone, and the second station 20 is a base station. The first station 10 communicates with the second station 20 over a plurality of radio bearers 12. The second station 20 thus has corresponding radio bearers 22, one for each of the radio bearers 12. Each radio bearer 12 has a receiving buffer 12r for holding protocol data units (PDUs) 11r received from the corresponding radio

bearer 22 of the second station 20. Each radio bearer 12 also has a transmitting buffer 12t for holding PDUs 11t that are awaiting transmission to the corresponding radio bearer 22 of the second station 20. A PDU 11t is transmitted by the first station 10 along a radio bearer 12 and received by the second station 20 to generate a corresponding PDU 21r in the receiving buffer 22r of the corresponding radio bearer 22. Similarly, a PDU 21t is transmitted by the second station 20 along a radio bearer 22 and received by the first station 10 to generate a corresponding PDU 11r in the receiving buffer 12r of the corresponding radio bearer 12.

[0005] For the sake of consistency, the data structures of each PDU 11r, 11t, 21r and 21t along corresponding radio bearer 12 and 22 are identical. That is, a transmitted PDU 11t generates an identical corresponding received PDU 21r, and vice versa. Furthermore, both the first station 10 and the second station 20 use identical PDU 11t, 21t data structures. Although the data structure of each PDU 11r, 11t, 21r and 21t along corresponding radio bearers 12 and 22 is identical, different radio bearers 12 and 22 may use different PDU data structures according to the type of connection agreed upon along the corresponding radio bearers 12 and 22. In general, though, every PDU 11r, 11t, 21r and 21t will have a sequence number 5r, 5t, 6r, 6t. The sequence number 5r, 5t, 6r, 6t is an m-bit number that is incremented for each PDU 11r, 11t, 21r, 21t. The magnitude of the sequence number 5r, 5t, 6r, 6t indicates the sequential ordering of the PDU 11r, 11t, 21r, 21t in its buffer 12r, 12t, 22r, 22t. For example, a received PDU 11r with a sequence number 5r of 108 is sequentially before a received PDU 11r with a sequence number 5r of 109, and sequentially after a PDU 11r with a sequence number 5r of 107. The sequence number 5t, 6t is often explicitly carried by the PDU 11t, 21t, but may also be implicitly assigned by the station 10, 20. For example, in an acknowledged mode setup for corresponding radio bearers 12 and 22, each transmitted PDU 11t, successful reception of which generates an identical corresponding PDU 21r, is confirmed as received by the second station 20. Ideally, the sequence numbers 5t maintained by the first station 10 for the PDUs 11t are identical to the corresponding sequence numbers 6r for the PDUs 21r that are maintained by the second station 20.

[0006] Hyper-frame numbers (HFNs) are also maintained by the first station 10 and the second station 20. Hyper-frame numbers may be thought of as high-order (i.e., most

significant) bits of the sequence numbers 5t, 6t, and which are never physically transmitted with the PDUs 11t, 21t. Exceptions to this rule occur in rare cases of special signaling PDUs 11t, 21t that are used for synchronization. In these cases, the HFNs are not carried as part of the sequence number 11t, 21t, but instead are carried in fields of the data payload of the signaling PDU 11t, 21t, and thus are more properly signaling data. As each transmitted PDU 11t, 21t generates a corresponding received PDU 21r, 11r, hyper-frame numbers are also maintained for received PDUs 11r, 21r. In this manner, each received PDU 11r, 21r, and each transmitted PDU 11t, 21t is assigned a value that uses the sequence number (implicitly or explicitly assigned) 5r, 6r, and 5t, 6t as the least significant bits, and a corresponding hyper-frame number (always implicitly assigned) as the most significant bits. Each radio bearer 12 of the first station 10 thus has a receiving hyper-frame number (HFN_R) 13r and a transmitting hyper-frame number (HFN_T) 13t. Similarly, the corresponding radio bearer 22 on the second station 20 has a HFN_R 23r and a HFN_T 23t. When the first station 10 detects rollover of the sequence numbers 5r of PDUs 11r in the receiving buffer 12r, the first station 10 increments the HFN_R 13r. On rollover of sequence numbers 5t of transmitted PDUs 11t, the first station 10 increments the HFN_T 13t. A similar process occurs on the second station 20 for the HFN_R 23r and HFN_T 23t. Ideally, the HFN_R 13r of the first station 10 should thus be synchronized with (i.e., identical to) the HFN_T 23t of the second station 20. Similarly, the HFN_T 13t of the first station 10 should be synchronized with (i.e., identical to) the HFN_R 23r of the second station 20.

[0007]

A security engine 14 on the first station 10, and a corresponding security engine 24 on the second station 20, together ensure secure and private exchanges of data exclusively between the first station 10 and the second station 20. The security engine 14, 24 is used for performing the obfuscation (i.e., ciphering, or encryption) of data held within a PDU 11t, 21t so that the corresponding PDU 11r, 21r presents a meaningless collection of random numbers to an eavesdropper. For transmitting a PDU 11t, the security engine 14 uses, amongst other inputs, an n-bit security count 14c and a security key 14k to perform the ciphering functions upon the PDU 11t. To properly decipher the corresponding PDU 21r, the security engine 24 must use an identical security count 24c and security key 24k. To start the ciphering upon the

radio bearers 12,22, the second station 20 has to send a "SECURITY MODE COMMAND" message to the first station 10. Each of the first station 10 and the second station 20 has a corresponding variable CIPHERING_STATUS 16, 26 respectively to record a ciphering status as "STARTED" or "NOT STARTED". For example, the variable CIPHERING_STATUS 26 is initially set to "NOT STARTED" before the ciphering is started between the first and second stations 10, 20. When the first station 10 receives the "SECURITY MODE COMMAND" command from the second station 20 that indicates that ciphering should be activated, the variable CIPHERING_STATUS 16 is set to "STARTED". The CIPHERING_STATUS 16 is initially set to "NOT STARTED" until the second station 20 sends the "SECURITY MODE COMMAND" message to the first station 10 for starting the ciphering. In addition, after the first station 10 is ready to perform the ciphering upon PDUs, the variable CIPHERING_STATUS 26 of the second station 20 will be set to "STARTED". That is, the variables CIPHERING_STATUS 16 and the CIPHERING_STATUS 26 are synchronized to make the ciphering between the first and second stations 10, 20 operate correctly. If there are a plurality of first stations 10 each having a specific variable CIPHERING_STATUS 16 to indicate the corresponding ciphering status between the first station 10 and the second station 20, the second station 20, therefore, has to establish a plurality of variables CIPHERING_STATUS 26 each being synchronized with one variable CIPHERING_STATUS 16 of each first station 10 for transmitting and receiving PDUs correctly.

[0008]

The security count 14c for a PDU 11t is generated by using the sequence number 5t of the PDU 11t as the least significant bits of the security count 14c, and the HFN_T 13t associated with the sequence number 5t as the most significant bits of the security count 14c. Similarly, the security count 14c for a PDU 11r is generated from the sequence number 5r of the PDU 11r and the HFN_R 13r of the PDU 11r. An identical process occurs on the second station 20, in which the security count 24c is generated using the sequence number 6r or 6t, and the appropriate HFN_R 23r or HFN_T 23t. The security count 14c, 24c has a fixed bit size, which is typically 32 bits. As the sequence numbers 5r, 6r, 5t, 6t may vary in bit size depending upon the transmission mode used, the hyper-frame numbers HFN_R 13r, HFN_R 23r, HFN_T 13t and HFN_T 23t must vary in bit size in a corresponding manner to yield the fixed bit

size of the security count 14c, 24c. For example, in a transparent transmission mode, the sequence numbers 5r, 6r, 5t, 6t are all 7 bits in size. The hyper-frame numbers HFN_R 13r, HFN_R 23r, HFN_T 13t and HFN_T 23t are thus 25 bits in size; combining the two together yields a 32 bit security count 14c, 24c. On the other hand, in an acknowledged transmission mode, the sequence numbers 5r, 6r, 5t, 6t are all 12 bits in size. The hyper-frame numbers HFN_R 13r, HFN_R 23r, HFN_T 13t and HFN_T 23t are thus 20 bits in size so that combining the two together continues to yield a 32 bit security count 14c, 24c.

[0009] As noted, the first station 10 may establish a plurality of radio bearers 12 with the second station 20. Each of these radio bearers 12 uses its own sequence numbers 5r and 5t, and hyper-frame numbers 13r and 13t. When establishing a new radio bearer 12, the first station 10 calculates an START value by considering the HFN_T 13t and HFN_R 13r of all currently established radio bearers 12, and selects the HFN_T 13t or HFN_R 13r having the highest value and add one to the value. The START value is stored in a variable START_VALUE_TO_TRANSMIT. Then, the variable START_VALUE_TO_TRANSMIT is sent to the second station 20 in a "RADIO BEARER SETUP COMPLETE" message. However, if the variable "CIPHERING_STATUS" is set to "NOT STARTED", the initial value is calculated based on the HFN_T 13t and HFN_R 13r of all currently established radio bearers 12, but is not used for initializing the HFN_T 13t and the HFN_R 13r for the new radio bearer 12. That is, the HFN_T 13t and the HFN_R 13r are initialized by the calculated initial value only when the variable "CIPHERING_STATUS" 16 is set to "STARTED". Generally speaking, The first station 10 then extracts the MSB_X of this highest-valued hyper-frame number 13r, 13t, increments the MSB_X by one, and uses it as the MSB_X for the new HFN_T 13t and HFN_R 13r for a newly established radio bearer 12 with a corresponding variable "CIPHERING_STATUS" set to "STARTED". Synchronization is then performed between the first station 10 and the second station 20 to provide the MSB_X to the second station 20 for the HFN_R 23r and HFN_T 23t.

[0010] However, the establishment of a new radio bearer 12 may generate a problem when considering the possibility of the variable CIPHERING_STATUS being set to "NOT STARTED". Please refer to Fig.2, which is a flow chart related to a prior art establishment of the radio bearer 12. Establishing a new radio bearer 12 has the

following steps.

[0011] Step 101:

[0012] The second station 20 transmits a "RADIO BEARER SETUP" message to the first station 10 for triggering an establishment of a new radio bearer 12;

[0013] Step 102: The first station 10 calculates a START value;

[0014] Step 103:

[0015] The first station 10 checks whether the variable CIPHERING_STATUS is set to "STARTED" or "NOT STARTED". If the status is "STARTED" for the new radio bearer 12, go to Step 104; otherwise, go to Step 105;

[0016] Step 104: Use the START value to initialize the HFNs related to the new radio bearers 12;

[0017] Step 105:

[0018] The first station 10 transmits a "RADIO BEARER SETUP COMPLETE" message, which contains the START value, to the second station 20 to inform the second station 20 that the new radio bearer 12 has been successfully established.

[0019] As mentioned above, when a new radio bearer is established, HFNs 13r and 13t will be initialized with the variable START_VALUE_TO_TRANSMIT if the CIPHERING_STATUS is set to "STARTED". However, when a new radio bearers 12 is created with the variable CIPHERING_STATUS set to "NOT STARTED", an initial value for the HFN_R 13r and HFN_T 13t is calculated, but no HFN 13r, 13t is initialized by the calculated value. Because the CIPHERING_STATUS is set to "NOT STARTED", ciphering is disabled, and the corresponding security count 14c is not maintained. In addition, the HFNs 13r, 13t for the new radio bearer 12, not having been initialized, are effectively random numbers. Consider the situation in which a great number of PDUs 11t are transmitted from the first station 10 to the second station 20, resulting in the related HFN_T 13t increasing in value. The first station 10 may later receive the "SECURITY MODE COMMAND" message from the second station 20, intending to start the ciphering. Because the HFN_R 13r and HFN_T 13t were not initialized when the

radio bearer 12 was established, the HFNs 13r, 13t are random and meaningless numbers. In addition, the HFNs 13r, 13t are not initialized when the "SECURITY MODE COMMAND" message has been transmitted and received. It can be expected, then, that the HFN_R 13r and HFN_T 23t are not synchronized, and that the HFN_R 23r and HFN_T 13t are also not synchronized. Consequently, when the "SECURITY MODE COMMAND" message is sent by the second station 20, a corresponding ciphering function fails along the new radio bearer 12 between the first station 10 and the second station 20 due to the unsynchronized HFNs for the new radio bearer 12 between the first and second stations 10, 20. Besides, the prior art does not teach or mention about initializing the HFNs of the ever established radio bearers when the first station 10 later receives the "SECURITY MODE COMMAND" message to start the ciphering operation. However, it is not reasonable trying to initialize HFNs by the variable START_VALUE_TO_TRANSMIT at this time to solve the above-mentioned problem since the variable START_VALUE_TO_TRANSMIT that stores the original calculated START value might have been altered owing to new establishments of other radio bearers between the first station 10 and the second station 20. That is, the original calculated START value of the target radio bearer might be lost when the first station 10 later receives the "SECURITY MODE COMMAND" message for the target radio bearer.

[0020] For the sake of ensuring secure data transmission, the second station 20 may also trigger a counter check procedure to perform a local authentication. The purpose of the procedure is to check that the amount of data sent in both directions, that is, from the second station 20 to the first station 10 and from the first station 10 to the second station 20, over a duration of the established radio bearer 12 is identical at the first and second stations 10, 20. The procedure is helpful for detecting a possible intruder. It is obvious that the security count 14c, 24c containing an HFN and an SN related to a PDU can be used to calculate total amount of transmitted data. Whether the ciphering is activated or not, the security count 14c, 24c, should be possible at all the times during the existence of the radio bearer 12. As mentioned above, the security count 14c is a random number when the variable CIPHERING_STATUS is set to "NOT STARTED" during establishment of the new radio bearer 12. Therefore, the counter check procedure will not function correctly for the new radio bearer12.

Summary of Invention

[0021] It is therefore a primary objective of the present invention to provide a method of initializing HFNs during establishment of a new radio bearer in a wireless communication system so as to maintain synchronization of the HFNs even if the ciphering has not been started.

[0022] Briefly summarized, the preferred embodiment of the present invention discloses a method for setting an initial hyper frame number (HFN) for a new radio bearer in a wireless communication system. The wireless communication system has a mobile unit, a base station, and a plurality of established radio bearers. The base station is used for transmitting a first control command to the mobile unit, and the first control command is used for triggering establishment of the new radio bearer between the mobile unit and the base station. Each established radio bearer between the mobile unit and the base station has a corresponding first HFN. The mobile unit generates a first value based on the first HFNs of established radio bearers wherein the first value is at least as great as the x most significant bits (MSB_x) of each first HFN. Each of the mobile unit and the base station sets the MSB_x of an initial HFN associated with the new radio bearer equal to the first value, regardless of the status of the CIPHERING_STATUS variable.

[0023] It is an advantage of the present invention that by initializing HFNs associated with a new radio bearer regardless of whether or not the ciphering is started or not for the new radio bearer, proper synchronization of the HFNs with the base station is ensured. It is a further advantage that this also leads to proper operation of a counter check procedure.

[0024] These and other objectives of the present invention will no doubt become obvious to those of ordinary skill in the art after reading the following detailed description of the preferred embodiment, which is illustrated in the various figures and drawings.

Brief Description of Drawings

[0025] Fig.1 is a simplified block diagram of a prior art wireless communications system.

[0026] Fig.2 is a flow chart related to a prior art establishment of the radio bearer.

[0027] Fig.3 is a flow chart related to establishment of the radio bearer shown in Fig.1 according to the method of the present invention.

Detailed Description

[0028] Please refer to Fig.1 and Fig.3. Fig.3 is a flow chart related to establishment of the radio bearer 12 shown in Fig.1 according to the method of the present invention. In the preferred embodiment, the establishment of the radio bearer 12 has following steps.

[0029] Step 201: The second station 20 transmits a "RADIO BEARER SETUP" message to the first station 10 for triggering an establishment of a new radio bearer 12;Step 202: The first station 10 calculates a START value;Step 203: The first station 10 uses the START value to initialize HFNs related to the new radio bearer 12, regardless of the state of the CIPHERING_STATUS variable;Step 204: The first station 10 transmits a "RADIO BEARER SETUP COMPLETE" message, which contains the START value, to the second station 20 to inform the second station 20 that the new radio bearer 12 has been successfully established.

[0030] The operation of the preferred embodiment is described as follows. When a new radio bearer 12, 22 is to be established, the second station 20 will send a "RADIO BEARER SETUP" message to the first station 10. When the first station 10 receives the "RADIO BEARER SETUP" message, the first station 10 calculates an initial value for the HFNs 13r, 13t first. Initially, there are no established radio bearers 12 and 22 between the first station 10 and the second station 20. The first station 10 thus establishes a radio bearer 12 with the second station 20. Therefore, the first station 10 must determine the initial value. The first station 10 references a non-volatile memory 17, such as a flash memory device or a SIM card, for a START value 18 and uses the START value 18 to generate and set the initial value for the HFN_T 13t and the HFN_R 13r, regardless of whether or not the variable "CIPHERING_STATUS" is "STARTED" or "NOT STARTED". That is, when the first station 10 is powered on, the START value 18 stored in the SIM card is used for initializing the HFN_T 13t and the HFN_R 13r for a new radio bearer in the preferred embodiment. Therefore, the START value is obtained with absence of the security counts and the integrity counts in the beginning as mentioned above. The start value 18 holds the x most significant bits (MSB_x) of a hyper-frame

number from a previous session along a radio bearer 12. Ideally, x should be at least as large as the bit size of the smallest-sized hyper-frame number (i.e., for the above example, x should be at least 20 bits in size). The MSB_x of the HFN_T 13t and the HFN_R 13r are set to the START value 18, and the remaining low order bits are set to zero. After the setting related to the new radio bearer 12 is done, the first station 10 will transmit a "RADIO BEARER SETUP COMPLETE" message to the second station 20. The variable START_VALUE_TO_TRANSMIT stores the START value 18 related to the newly created radio bearer, and is included in the "RADIO BEARER SETUP COMPLETE" message. In doing so, the first station 10 transmits the START value 18 embedded in the "RADIO BEARER SETUP COMPLETE" message to the second station 20 for use as the HFN_R 23r and the HFN_T 23t. In this manner, the HFN_T 13t is synchronized with the HFN_R 23r, and the HFN_T 23t is synchronized with the HFN_R 13r when the new radio bearer 12 is established.

[0031]

As noted, the first station 10 may have established a plurality of radio bearers 12 with the second station 20. Each of these radio bearers 12 uses its own sequence numbers 5r and 5t, and hyper-frame numbers 13r and 13t. When establishing a new radio bearer 12, the first station 10 considers the HFN_T 13t and HFN_R 13r of all currently established radio bearers 12, and selects the HFN_T 13t or HFN_R 13r having the highest value. The first station 10 then extracts the MSB_x of this highest-valued hyper-frame number 13r, 13t, increments the MSB_x by one, and uses it as a calculated START value 18 for the MSB_x for the new HFN_T 13t and HFN_R 13r for a newly established radio bearer 12. The HFN_T 13t and HFN_R 13r for the newly established radio bearer 12, which is being established in response to the "RADIO BEARER SETUP" message from the second station 20, are initialized using this calculated START value 18, regardless of the state of the CIPHERING_STATUS variable 16. The first station 10 then embeds the calculated START value 18 in a "RADIO BEARER SETUP COMPLETE" message, which is transmitted to the second station 20. Synchronization is thus ensured between the first station 10 and the second station 20 to provide the MSB_x to the second station 20 for the HFN_R 23r and HFN_T 23t. The HFN_T 13t is synchronized with the HFN_R 23r, and the HFN_T 23t is synchronized with the HFN_R 13r when the new radio bearer 12 is established, regardless of whether or not the variable CIPHERING_STATUS 16 is set to "STARTED" or "NOT

STARTED". Consequently, the security counts 14c, 24c in the preferred embodiment are initialized and synchronized when a new radio bearer 12 is established.

[0032] When the second station 20 activates the counter check procedure to perform a corresponding authentication, the counter check procedure works because the security counts 14c, and 24c are maintained with HFNs that are guaranteed to be initialized and synchronized from the establishment time of the new radio bearer 12, 22. That is, the HFNs 13r, 13t are initialized even though the variable CIPHERING_STATUS is set to "NOT STARTED" when the new radio bearer 12 is established, indicating that no ciphering is to be performed along the new radio bearer 12. Therefore, the security counts 14c, and 24c are initialized with the synchronized HFNs so that the counter check procedure can check the amount of data transmitted between the first station 10 and the second station 20 with the help of initialized security counts 14c, and 24c, even though the ciphering has not yet been activated.

[0033] In contrast to the prior art, the method according to the present invention initializes the HFNs when a new radio bearer is established, regardless of the state of the CIPHERING_STATUS variable. That is, an initial value is calculated and is assigned to the HFNs related to the new radio bearer, regardless of whether the CIPHERING_STATUS is set to "STARTED" or "NOT STARTED". The HFNs related to the new radio bearer are thus synchronized and initialized after the establishment of the new radio bearer so that the counter check procedure requiring a security count will work normally even though the ciphering not activated.

[0034] Those skilled in the art will readily observe that numerous modifications and alterations of the device may be made while retaining the teaching of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.